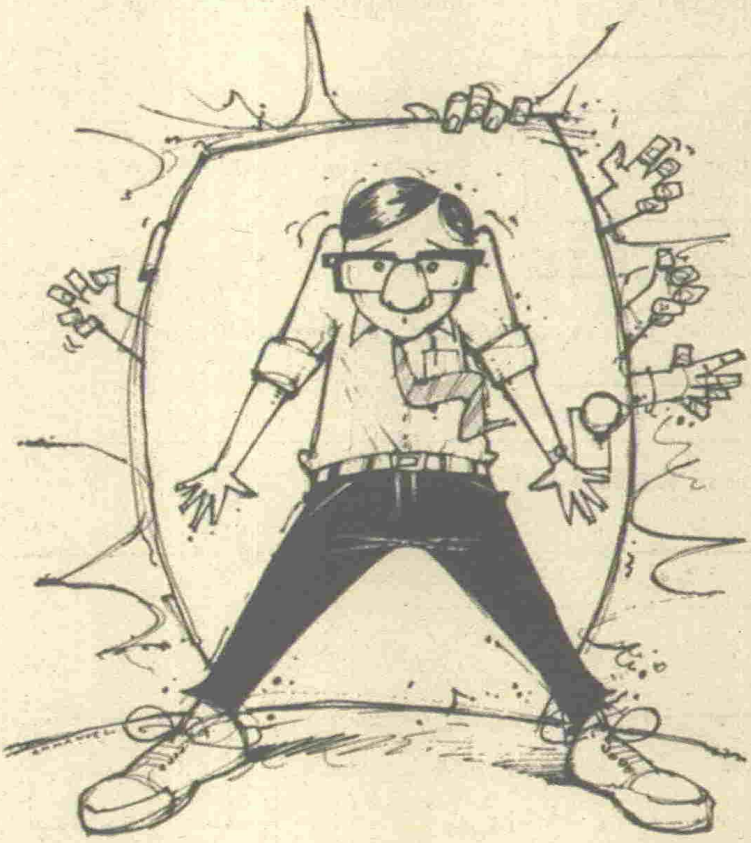
นงเยาว์ เชื่อมจอหอ

SOFT MAIL

การตรวจสอบและทำลาย ไวรัสไมเคิลแองเจลโล

ค้นพบแล้ว...วิธีการตรวจสอบและทำลายไวรัสไมเคิลแองเจลโล คุ้มครองความปลอดภัยให้กับข้อมูลของคุณ



การตรวจสอบไวรัสไมเคิลแองเจลโลทั้งในฮาร์ดดิสก์และฟลอปปี้ดิสก์ทำได้หลายวิธี เช่น

1.1 ใช้นอร์ตันดิสก์ด็อกเตอร์ (NDD.EXE) ซึ่งเมื่อรันที่ DOS prompt จะมีเมนูขึ้นมาดังรูปที่ 1

ให้เลือก Diagnose disk ซึ่งจะแสดงเมนูเพื่อให้เลือกไดรฟ์ที่จะตรวจสอบ ดังรูปที่ 2

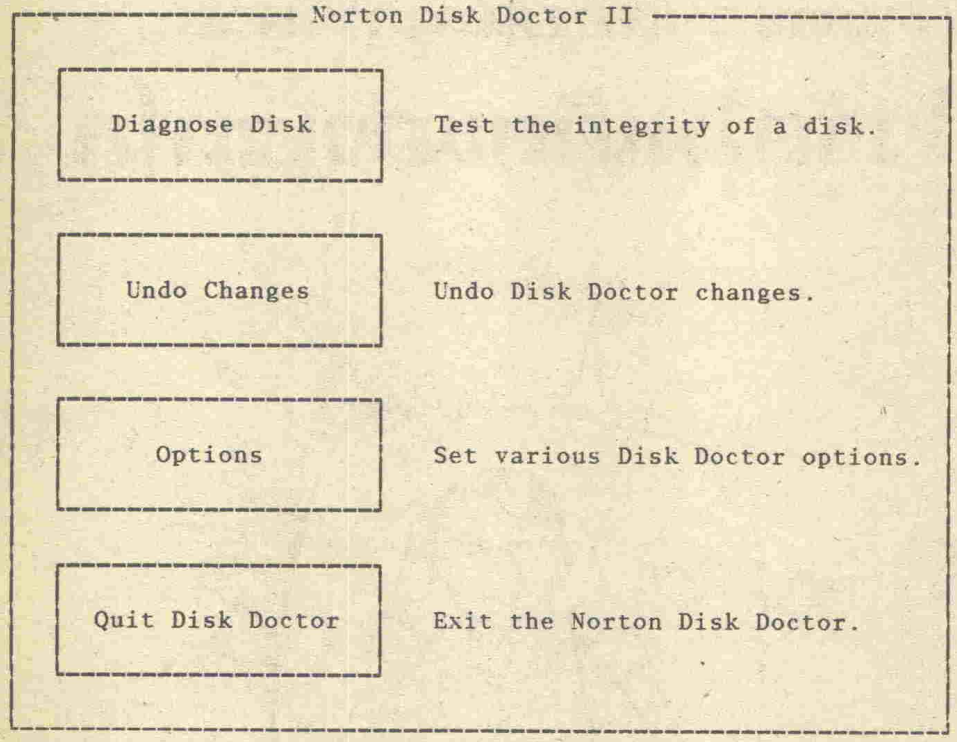
หากเลือกไดรฟ์ A: จะมีคำสั่งให้ใส่แผ่นดิสก์เข้าไปในช่อง A : จากนั้นโปรแกรมจะเริ่มทำการตรวจสอบบูตเรคอร์ดซึ่งเป็นส่วนที่ไวรัสไมเคิลแองเจลโลซ่อนตัวอยู่ ถ้าหากมีไวรัสนี้ซ่อนตัวอยู่จริงโปรแกรมก็จะแสดงข้อความบ่งบอกถึงความผิดปกติออกมาดังรูปที่ 3

หากต้องการทำลายไวรัสนี้ให้ตอบตกลง (Yes) โปรแกรมจะถามความต้องการว่าจะให้เก็บไฟล์ชื่อ NDDUNDO.DAT (ซึ่งสร้างสำรองไว้ในกรณีเปลี่ยนใจไม่อยากแก้ไขบูตเรคอร์ด) ไว้ด้วยหรือไม่ หากต้องการเก็บไว้และเก็บไว้ที่ไดรฟ์ใด แต่ถ้าไม่ต้องการเก็บไฟล์นี้ไว้ให้ตอบ Cancel แล้วโปรแกรมก็จะดำเนินการฆ่าไวรัสให้ดังรูปที่ 4

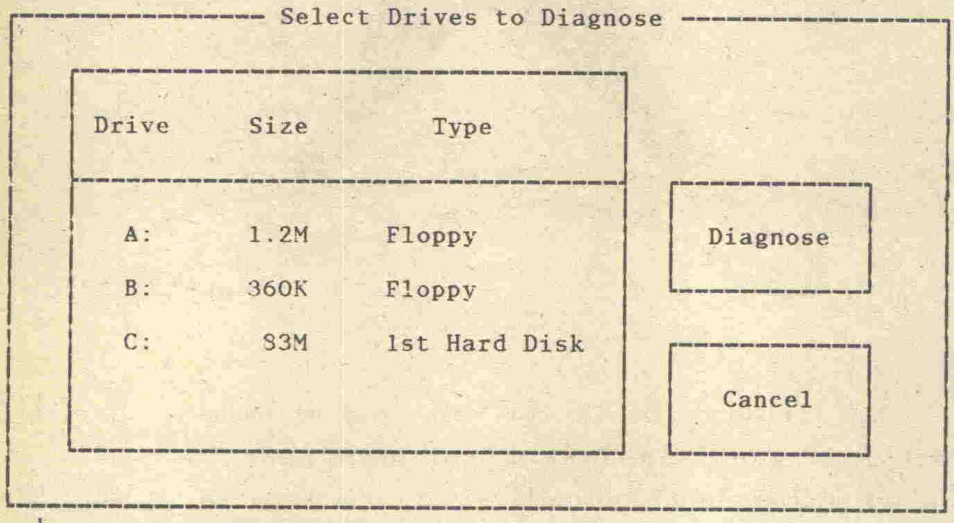
1.2 ใช้โปรแกรม DEBUG ซึ่งสามารถตรวจสอบไวรัสนี้ได้ทั้งในหน่วยความจำและในแผ่นดิสก์โดยใช้วิธีการค้นหารหัสของไวรัส (Virus Signature) ตัวนี้มีวิธีการดังนี้

1.2.1 กรณีตรวจสอบไวรัสในหน่วยความจำ ให้รันโปรแกรม DEBUG ที่ DOS prompt แล้วพิมพ์ข้อความต่อไปนี้เพื่อค้นหารหัสของไวรัส ซึ่งจะอยู่ที่ส่วนท้ายของหน่วยความจำ กรณีที่เครื่องมีหน่วยความจำ (Conventional memory) เป็น 640 กิโลไบต์ ให้พิมพ์

-s 9000:0 ffff d2 b9 01 00 b8 09 03 8b 36 08 00 83 fe 03 (กดแป้น Enter) ซึ่งถ้าในหน่วยความจำมีไวรัสอยู่ดีบักก็จะแสดงตำแหน่งที่พบออกมา เช่น 9000:F94C หรือ 9000:FB4C เป็นต้น แต่ถ้าในหน่วยความจำไม่มีไวรัสตัวนี้อยู่ดีบักก็จะไม่พิมพ์อะไรออกมา



รูปที่ 1 แสดงโปรแกรม Norton Disk Doctor II



รูปที่ 2 แสดง MENU ภายใน Diagnose disk

1.2.2 กรณีตรวจหาไวรัสในแผ่นดิสค์ให้โหลดบูตเรคอร์ด (จำนวน 512 ไบต์) ของดิสค์แผ่นนั้นมาเก็บไว้ในหน่วยความจำแล้วค้นหารหัสของไวรัสในลักษณะเดียวกับข้อ 1.2.1 เช่น กรณีตรวจสอบดิสค์ในไดรฟ์ A: ให้พิมพ์ -L 100 0 0 1 (กดแป้น Enter) พิมพ์ต่อด้วย -S 100 2ff d2 b9 01 00 b8 09 03 8b 36 08 00 83 fe 03 (กดแป้น Enter) ซึ่งหากแผ่นดิสค์นั้นติดไวรัสตัวนี้ดีบักก็จะแสดงตำแหน่งที่พบออกมา เช่น XXXX:024C เป็นต้น

หมายเหตุ เพื่อความสะดวกในการใช้งานด้วยดีบักจึงได้เขียนเป็นแบตช์ไฟล์ชื่อ MIK.BAT ดังรูปที่ 5

แบตช์ไฟล์นี้สามารถตรวจหาการติดเชื้อได้ทั้งในเมมโมรีและดิสเกตต์ของไดรฟ์ A-C โดยมีรูปแบบดังนี้ ให้พิมพ์ MIK (กด Enter) จะเป็นการตรวจหาไวรัสในหน่วยความจำ แต่ถ้ามีการระบุชื่อไดรฟ์ด้วยจะเป็นการตรวจหาไวรัสในแผ่นดิสค์ที่อยู่ในไดรฟ์นั้น ๆ การจะรันแบตช์ไฟล์นี้ได้จะต้องมีโปรแกรมดีบักอยู่ในไดเรคทอรีเดียวกันกับแบตช์ไฟล์นี้ มิฉะนั้นต้องเซตพาธให้ด้วย

1.3 การใช้กลุ่มโปรแกรมตรวจสอบจำนวนหน่วยความจำของเครื่อง เช่น

1.3.1 ใช้ Memory mapping (MEM.EXE) ของ DOS เวอร์ชัน 4 ขึ้นไป

```
C:\ >MEM (กด Enter)
653312 bytes total   conventional
memory <- - - -  638 x 1024 ไบต์
```

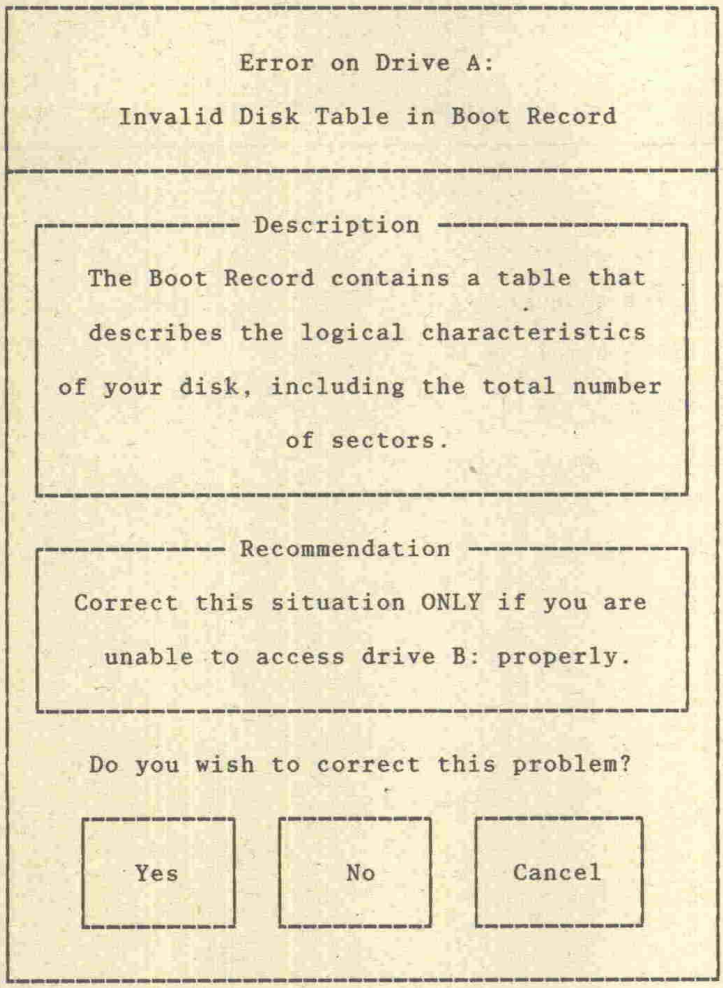
1.3.2 CHKDSK.EXE ของ DOS

```
C:\ > CHKDSK (กด Enter)
653312 total bytes
memory <- - - -  638 x 1024 ไบต์
598320 bytes free
```

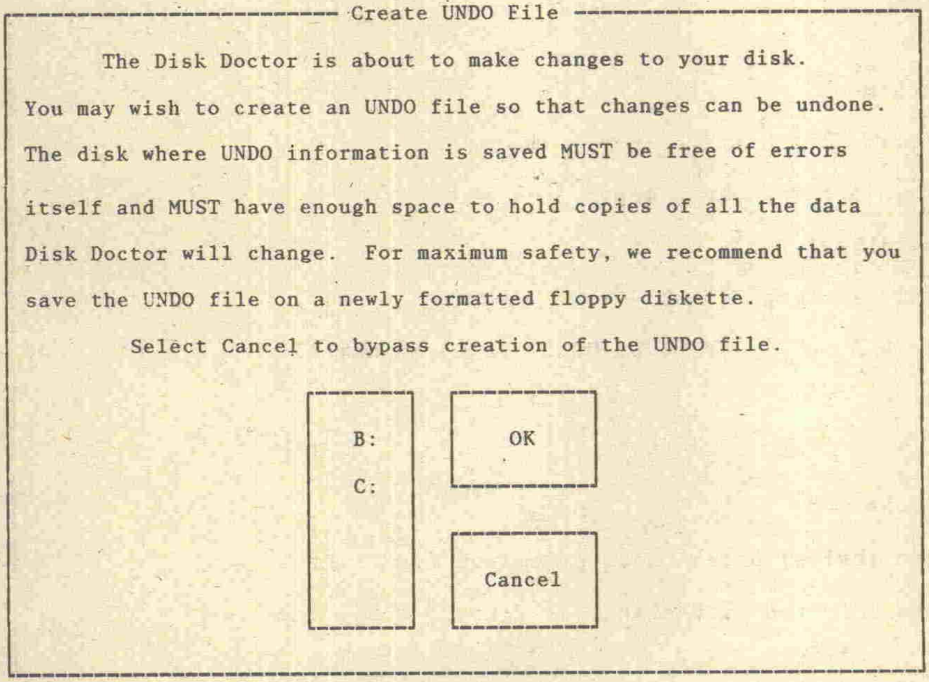
1.3.3 Memory Information ในชุดของ PCTOOLS (MI.EXE) ซึ่งจะให้ข้อมูลดังนี้

```
C:\ >MI (กด Enter)
Conventional memory.
Total : 638 k <- - - -  หายไป 2 กิโลไบต์
Largest executable program : 584 k
```

1.3.4 ใช้ PCTOOLS.EXE โดยเรียกโปรแกรม PCTOOLS จากนั้นกดแป้นฟังก์ชันคีย์ F3 ตามด้วยแป้น



รูปที่ 3 แสดงผลการตรวจสอบความผิดปกติ ซึ่งเกิดจากไวรัส Michaelangelo



รูปที่ 4 แสดง MENU ของการที่จะสร้างหรือไม่สร้างไฟล์ NDDUNPO.DAT

ตัวอักษร I เพื่อเลือก System Information Service ดูผลลัพธ์ จะเห็นเป็น

```
Total memory reported by Dos
-638 k <- - - - หายไป 2 กิโลไบต์
PC Tools has found the total memory
to be -640 k
```

1.3.5 System Information (SI.EXE) ของ Peter Norton

```
C:\ >SI (กด Enter)
DOS reports 638 K-bytes of memory
<— หายไป 2 กิโลไบต์
```

1.4 ใช้โปรแกรมตรวจสอบและฆ่าไวรัสนี้โดยเฉพาะ เช่น MIK.EXE ของบริษัท อาร์แอนด์ดี คอมพิวเตอร์ ซึ่งมีวิธีใช้งานดังนี้ MIK <ชื่อ Drive> <Option> เช่น MIK C: เป็นการตรวจหาและทำลายใน Drive C: หรือ MIK A: /M เป็นการตรวจหาในแผ่นฟลอปปี้ดิสค์ในช่อง A จำนวนหลาย ๆ แผ่นติดต่อกัน แต่ถ้าหาไม่ได้ก็ใช้นอร์ตันดิสค์ดือกเตอร์ดังกล่าวแล้วก็ได้

ป้องกันไวรัสอย่างไร

1. มีไบออสบางยี่ห้อเช่นของ AMI ที่สามารถกำหนดไม่ให้มีการเขียนฮาร์ดดิสค์พาร์ติชันหรือบูตเซกเตอร์ก่อน

รูปที่ 5 แสดงแบตช์ไฟล์ชื่อ MIR.BAT

```
@echo off
      cls
      echo          *** Michaelanglelo Virus scanner ***
      echo                Format: MIK [drive name]
   rem ---- Set drive: A = 0, B = 1, C = 2 ----
   rem ---- Check only memory if not spacefic disk driye ----
      set drv=NO
      if (%1) == (a)  set drv=0
      if (%1) == (a:) set drv=0
      if (%1) == (A)  set drv=0
      if (%1) == (A:) set drv=0
      if (%1) == (b)  set drv=1
      if (%1) == (b:) set drv=1
      if (%1) == (B)  set drv=1
      if (%1) == (B:) set drv=1
      if (%1) == (c)  set drv=2
      if (%1) == (c:) set drv=2
      if (%1) == (C)  set drv=2
      if (%1) == (C:) set drv=2
      if (%drv%) == (NO) goto :chkmem
   rem ---- Check virus in diskette in A-C drive ----
   rem ---- Load boot sector of target disk into memory ----
      echo l 0100 %drv% 0 1 >chkmik.dat
   rem ---- search Virus Signature in target disk ----
      echo s 0100 02ff D2 B9 01 00 B8 09 03 8B 36 08 00 83 FE 03 >>chkmik.dat
      echo q >>chkmik.dat
      echo
      debug <chkmik.dat >dismik.dat
      echo If DEBUG shows the address(es) after  search command (-s ...),
      echo It means your diskette infected Michaelanglelo Virus.
```

```
      echo
      type dismik.dat
:chkmem
   rem ---- search virus in memory ----
   rem ---- start at address  7000:0  in   512 KB RAM memory micro.
   rem                        9000:0  in   640 KB RAM memory micro.
   rem                        A000:0  in > 640 KB RAM memory micro.
   rem                        B000:0  in > 640 KB RAM memory micro.
   rem ---- and display to screen if found ----
      echo s 7000:0 FFFF D2 B9 01 00 B8 09 03 8B 36 08 00 83 FE 03 >chkmik.dat
      echo s 9000:0 FFFF D2 B9 01 00 B8 09 03 8B 36 08 00 83 FE 03 >>chkmik.dat
      echo s A000:0 FFFF D2 B9 01 00 B8 09 03 8B 36 08 00 83 FE 03 >>chkmik.dat
      echo s B000:0 FFFF D2 B9 01 00 B8 09 03 8B 36 08 00 83 FE 03 >>chkmik.dat
   rem ---- call debug progarm ----
      echo q >>chkmik.dat
      echo
      debug <chkmik.dat >dismik.dat
      echo If DEBUG shows the address(es) after any search command (-s ...),
      echo It means your memory infected Michaelanglelo Virus.
      echo
      type dismik.dat
:end
   rem ---- delete Environment variable and Data file (.dat) ----
      del chkmik.dat >NUL:
      del dismik.dat >NUL:
      set drv=
   rem  ---- END ----
```

ได้รับอนุญาต ดังนั้นจึงควรติดตั้งให้เป็น Enable ไว้เสมอ เพราะเมื่อนำแผ่นฟลอปปี้ดิสก์ที่มีไวรัสนี้อยู่ไปบูตระบบ ไวรัสจะแพร่ไปติดฮาร์ดดิสก์ทันที ซึ่งในกรณีเช่นนี้ให้ตอบ N แล้วจึงไปทำลายไวรัสที่ติดอยู่ในแผ่นฟลอปปี้ดิสก์เสียดังรูปที่ 6 หรือติดตั้งไวรัสการ์ดที่มีการป้องกันการเขียนฮาร์ดดิสก์พาร์ติชันหรือบูตเซกเตอร์ซึ่งก็จะให้คำเตือนในลักษณะเดียวกันนี้

2. มีไบออสบางยี่ห้อที่สามารถตั้งควิ๊กบูต (Quick Boot) ได้ก็ให้ติดตั้งไว้ ทั้งนี้เพื่อป้องกันการลืมหรือใส่แผ่นค้างไว้ในช่อง A ซึ่งแผ่นนั้นอาจมีไวรัสชนิดนี้หรือบูตเซกเตอร์ไวรัสตัวอื่น ๆ ติดอยู่ก็ได้ เมื่อเผลอไปกด 3 ปุ่ม (Ctrl-Alt-Del) เข้าเครื่องอาจจะบูตจากแผ่นที่ใส่ไว้ก็ได้ ทำให้ติดไวรัสไป (ควิ๊กบูต หมายถึง การบูตที่กำหนดให้ไม่ต้องมาอ่านไดรฟ์ A: หรือ B: ก่อนที่จะอ่าน Drive C: ทำให้ประหยัดเวลามาก เช่น กรณีไบออสของ QUADTEL Corp.)

3. ไม่ควรบูตระบบด้วยแผ่นดิสก์เกตต์และหมั่นตรวจสอบแผ่นดิสก์เกตต์ทั้งหมดที่มีอยู่ เพราะแม้ว่าแผ่นดิสก์นั้นจะเป็นแผ่นที่ไม่สามารถบูตได้ก็ตาม แต่ก็สามารถแพร่ไปสู่ฮาร์ดดิสก์ได้ และเมื่อฮาร์ดดิสก์นั้นติดไวรัสตัวนี้ไปแล้ว หากนำแผ่นฟลอปปี้ดิสก์ที่ไม่ได้ปิดแผ่นป้องกันการเขียนทับมาใช้กับเครื่องนี้ก็จะติดเชื้อหมดทุกแผ่น

4. การแก้ปัญหาเฉพาะหน้าในวันที่ 6 มีนาคม ซึ่งเป็นวันที่ไวรัสนี้ถูกสั่งให้ทำลายข้อมูลนั้น อาจจะใช้วิธีเปลี่ยนวันที่/เดือน ให้เป็นวันอื่นแทนการปิดเครื่องหรือหยุดทำงานไป 1 วันก็ได้ โดยใช้ดอสเวอร์ชัน 3 ขึ้นไป ซึ่งสามารถเซตซีมอสคล็อกได้โดยตรง

```
Hard Disk Virus Protection
Attempt to modify hard disk partition table or boot sector
Would you like to allow this midification ?
Press Y/N/D  (Y = Yes, N = NO, D = Disable virus protection
```

รูปที่ 6 แสดง Hard Disk Virus Protection

แต่วิธีนี้จะใช้ไม่ได้กับไวรัสที่ไม่รู้วันที่จะแผลงฤทธิ์หรือแม้แต่ไวรัสตัวนี้ถ้าถูกปรับปรุงให้ไปทำลายในวันอื่น

5. การเสียหายที่เกิดจากไวรัสตัวนี้เท่าที่เกิดกับตัวเองหรือคนใกล้เคียงคือ

5.1 ตารางพาร์ติชัน, บูตเรคอร์ด, ตาราง FAT, ไดเรคทอรีเสียหาย ทำให้สูญเสียข้อมูลหมดทุกไฟล์รวมทั้งไฟล์ระบบที่ซ่อนไว้ เช่น IO.SYS, MSDOS.SYS ทำให้ไม่สามารถบูตเครื่องจากฮาร์ดดิสก์ได้ (ซับไดเรคทอรีก็ถูกกลบไปด้วยโดยอัตโนมัติ)

5.2 มีข้อมูลขยะเกิดขึ้นในฮาร์ดดิสก์เป็นจำนวนมากหรือ

5.3 เกิดการซ้อนทับของกันซับไดเรคทอรีไปเรื่อย ๆ เช่น เดิมมีแต่เฉพาะ C:\Norton แต่ต่อมากลายเป็น C:\Norton\Norton\Norton... ไปเรื่อย ๆ และไม่สามารถลบซับไดเรคทอรีนี้ทิ้งได้เลย

5.4 แผ่นจานแม่เหล็กของฮาร์ดดิสก์ถูกครูดโดยหัวอ่านทำให้ไม่สามารถเล่นเครื่องได้อีกเลยและต้องเปลี่ยนแผ่นจานแม่เหล็กใหม่ แต่ข้อนี้ไม่กล้าสรุปตรง ๆ ว่าเกิดจากไวรัสตัวนี้หรือเกิดจากการขนย้ายเครื่อง แต่เหตุการณ์นี้เกิดขึ้นหลังวันที่ 6 มีนาคม และตรวจสอบพบไวรัสตัวนี้อยู่ในหน่วยความจำด้วย โดยหลังจากที่กำลังแปลกใจว่าทำไมหน่วยความจำถึงหายไป 2 กิโลไบต์ สักครู่ต่อมาเครื่องก็แฮงไปเลย